

FEB 26 2007

REMARKS

Claims 1-25 were withdrawn from consideration. The Examiner entered a new grounds of rejection for Claims 26-50. Claims 26-50 are now rejected under 35 U.S.C. 102(e) as being anticipated by Brewer (USP 6,922,785).

Brewer describes a network interface card that has built in encryption hardware. "When the packet is received at a data processing system equipped in a similar manner as the sending data processing system, the decryption algorithm indicated by the flag in the packet header is applied to the data using decryption hardware built on the network interface card. The decrypted data is then sent to re-assembly logic for rebuilding the original message from the transmitted packets. Once the message is rebuilt, it is sent to a computer memory via a system bus for further processing. If the receiving data processing system is not equipped with a similar network interface card, it is still possible to decrypt the message if suitable software is provided. By using encryption and decryption hardware built-on the network interface card, the central processor of a data processing system is freed from the responsibility of performing encryption and decryption and can carry out other computational tasks in a timely manner" (column 2, lines 1-18). However, Brewer does not teach or suggest any security control indicator in the frame. Brewer also does not teach or suggest any security association identifiers associated with the frame. Furthermore, Brewer does not teach or suggest any algorithm information contained in any entry in a security database.

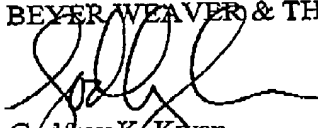
The material cited by the Examiner in column 2, lines 1-5 in fact explicitly states that the decryption algorithm is indicated "by the flag in the packet header." (column 2, line 4) The network card in Brewer uses the "decryption algorithm" is "indicated by the flag in the packet header" (column 2, line 4) and not any security control indicator in the frame. By contrast, the independent claims 26, 36, and 48 do not teach or suggest a variety of elements recited in the independent claims. For example, Brewer does not teach or suggest any "security control indicator in the frame" or any "security association identifiers associated with the frame" to identify an entry in a "security database." Brewer also does not teach or suggest using "algorithm information included in the entry in the security database."

More detail about Brewer's network interface card is provided in Figure 3. Figure 3 in Brewer is an exemplary block diagram of a network interface card that includes encryption and

decryption hardware. The network interface card does not include any security database. The Examiner may try to argue that control memory 306 or a computer memory itself could have a security database. However, Brewer states that control memory 306 is only used with segmentation and reassembly logic. "Segmentation and Re-assembly logic 304 performs these tasks with the help of control memory 306." (column 3, lines 53-54) No security association database is used. No algorithm information is included in an entry in the security database. No security association identifiers associated with the frame identify an entry in the security database.

In light of the above remarks relating to independent claims, the remaining dependent claims are believed allowable for at least the reasons noted above. Applicants believe that all pending claims are allowable and respectfully request a Notice of Allowance for this application from the Examiner. Should the Examiner believe that a telephone conference would expedite the prosecution of this application, the undersigned can be reached at the telephone number set out below.

Respectfully submitted,
BEYER WEAVER & THOMAS, LLP



Godfrey K. Kwan
Reg. No. 46,850

P.O. Box 70250
Oakland, CA 94612-0250
(510) 663-1100